Issues in Information Systems
Volume 26, Issue 3, pp. 377-386, 2025

DOI: https://doi.org/10.48009/3_iis_2025_2025_130

Strengthening cybersecurity education: The urgent need to integrate maritime cybersecurity into cyber programs

Karen Paullet, *Robert Morris University, paullet@rmu.edu*

Abstract

The maritime industry has undergone significant transformation as ships and ports have networks of digital systems which control navigation and cargo tracking. Approximately 90% of global commerce trade travels by sea. The increasing connectivity of maritime systems and the threat of cyberattacks have made cybersecurity a priority for the maritime industry. Maritime cybersecurity is a critical component of global trade and security. This research aims to justify the inclusion of maritime cybersecurity in university cybersecurity curricula.

Keywords: maritime cybersecurity, cybersecurity, cyberattacks, cybersecurity programs, maritime

Introduction

Maritime refers to anything related to the sea, especially navigation, shipping or marine activities. The maritime industry is a force in the global economy and is responsible for 90% of the world's trade and its activities encompass national security, international relations and the protection of the marine ecosystem (Nautic, 2025). The shipping industry transports and delivers approximately 11 billion tons of global trade volume annually while using only 50,000 merchant vessels to do so. The maritime industry's global network serves as the backbone of supply chain resilience. Interruptions to maritime transportation can cause port closures, vessel incidents or geopolitical pressures which can cause a domino effect throughout the global economy. Modern supply chains require physical infrastructure, sophisticated logistics networks, real-time tracking systems and contingency planning to maintain their resilience in case of disruption. The increasing connectivity of maritime systems and the threat of cyberattacks have made cybersecurity a priority for the maritime industry.

Over 95% of cargo entering the U.S. does so by ship and port operations which accounts for over 5 trillion in annual economic activity. Since early 2000's, ports have increasingly come to rely on automated forms of information and operational technology (IT and OT). This technological dependence has created vulnerabilities that could cripple the U.S. in the event of a cyberattack (Varley, et.al, 2024). In March 2024, the MV Dali hit the Key Bridge in Baltimore, MD, blocking the entrance to one of America's busiest ports and causing billions of dollars' worth of damage. Later in July 2024, a computer update administered by cybersecurity firm Crowdstrike disabled Windows services worldwide which led to chaos at airports and disrupted critical systems to include port facilities (Varley, et.al, 2024).

A crucial weakness in our defense against the increasing number of cyberthreats is revealed by the necessity of developing maritime cybersecurity education. The maritime industry faces cybersecurity issues that

traditional cybersecurity programs have not yet addressed as ships become more automated and ports embrace smart technologies. Cyberattacks have jeopardized international supply chains, interfered with port operations and compromised ship navigation systems. A fundamental part of academic cyber curricula should include maritime cybersecurity. There are several benefits that go beyond the classroom when maritime cybersecurity is incorporated into existing cybersecurity programs. By exposing students to the particular difficulties of safeguarding maritime infrastructure, this specialized focus enhances conventional academic institutions but also meets a pressing global need as maritime operations become more digitalized. Due to the shipping industry's significance to global trade, knowledge of maritime cybersecurity is crucial for safeguarding vital supply chains, national security and global trade. These improved programs strengthen the resilience of global maritime infrastructure and protect international trade by training cybersecurity professionals who comprehend both digital threats and maritime operations.

In an increasingly digitized maritime industry, expertise in cybersecurity represents a competitive advantage. Graduates who possess specialized knowledge in maritime cybersecurity will stand out from the competition. While traditional maritime education provides a foundation, the ability to understand and address cybersecurity challenges has become a distinguishing qualification. One that positions students at the forefront of the industry's digital transformation. This specialized knowledge is particularly valuable as shipping companies and ports intensify their focus on protecting critical infrastructure from cyber threats.
RQ1: How can implementing maritime cybersecurity into university curricula improve the preparedness and expertise of students studying cybersecurity?

Literature review

Research in the maritime sector shows that the fight against malware attacks is becoming more and more intense. In just ten years (2010–2020), a thorough analysis by Meland et al. (2021) found over 46 recorded malware-related maritime cyberattacks. It is not by accident that malware is so common; these attacks are a calculated tactic used by cybercriminals who are aware of the particular weaknesses in the maritime industry (Mrakovic, et.al. 2019). The most common attack vector in maritime cybersecurity breaches is malware, which gives hackers a flexible way to compromise vital systems like port infrastructure and ship navigation (Alcaide, et.al. 2020). The need for immediate attention to maritime cybersecurity in operational and educational contexts is highlighted by this pattern of malicious activity.

With its digital transformation accelerating at a never-before-seen rate, the maritime industry finds itself at a crucial technological crossroads. As indicated by P.T. International (2021) the technological market for the industry is expected to grow significantly, rising from the initial $279 billion forecast to $345 billion by 2030. This increase is indicative of a fundamental change in maritime operations, as digitization affects all facets of the sector. With the integration of satellite communications, IoT-enabled infrastructure, and increasingly autonomous systems, modern ships and ports function as complex digital ecosystems (Alquarashi, et.al. 2022).

A paradox is revealed by this digital revolution as cybersecurity protocols and education have not kept up with the maritime industry's rapid adoption of new technologies. Global maritime operations are seriously vulnerable as a result of this disconnect between security readiness and technology adoption. Individual assets as well as the entire maritime infrastructure that supports international trade are at risk due to the striking disparity between significant digital investments and insufficient cybersecurity measures. The urgent need for thorough maritime cybersecurity education and training programs is highlighted by this mismatch between technological advancement and security preparedness.

Overlaying these operational considerations is a sophisticated regulatory framework. Vessel security operates within a matrix of international laws, maritime conventions, and industry standards. This regulatory environment creates a complex compliance landscape that vessels must navigate while maintaining effective security measures. The challenge lies in balancing these various requirements while ensuring practical, implementable security protocols that crew members can consistently follow. A complex regulatory framework sits on top of these operational considerations. International laws, maritime conventions, and industry standards form the framework within which vessel security functions. Vessels must navigate a challenging compliance landscape created by this regulatory environment while upholding efficient security measures (Li, et.al., 2024).

At a 7.3% annual growth rate, the port security market is predicted to experience explosive growth, reaching an astounding $173.59 billion by 2031. This indicates that the maritime industry's perspective on security investments has fundamentally changed. This increase in investment reflects the complexity of contemporary ports, which are now complex digital hubs where physical security and cybersecurity are linked. A crucial realization is highlighted by the notable market expansion as ports are now essential nodes in the global digital infrastructure that demand state-of-the-art security solutions and not just places for the transit of goods. Ports' security requirements are evolving beyond conventional physical barriers to include comprehensive cyber-physical protection systems as they continue to adopt automation, artificial intelligence, and IoT technologies. This expanding market reflects the maritime industry's dedication to creating robust, secure infrastructure that can withstand new threats to global trade in a time when a single security breach can cause global trade disruptions (M. Intelligence, 2024).

Maritime Incidents

In 2025, modern ships' digital architecture relies heavily on the separation of information technology (IT) and operational technology (OT) systems, which have different but related functions. IT systems are largely responsible for business operations and data management, which includes everything from cargo documentation and fleet management software to crew emails and passenger records. These systems allow business-critical information to flow between ships and shoreside operations. OT systems serve as the technological foundation for the physical operations of the vessel. From navigation and engine management to navigation and engine controls, these systems regulate and keep an eye on vital shipboard operations. OT systems, which were previously isolated, are now more networked and interconnected, which brings with it both new vulnerabilities and new efficiencies (Marpoint, 2024). There has been a surge in maritime cyber incidents in 2024. Over 1,800 vessels were targeted in the first half of the year alone. Advanced attacks include:

- Command and Control Attacks which gives access to the ships systems for data theft and operational disruption
- Botnet Exploits that leverage IoT devices to spread malware across fleets
- AI-Powered Threats which are highly targeted and evasive attacks that challenge traditional defenses.

It is important to note that while advanced attacks exist, phishing remains a significant threat by exploiting human error to breach systems (Marpoint, 2024). Critical maritime infrastructure can become paralyzed by digital vulnerabilities, as demonstrated by the 2018 cyberattack on the Port of Barcelona. Real-world operational disruptions resulted from what started as an IT system breach. The event demonstrated the extent to which physical port operations and digital systems are now intertwined (Ilascu, 2018).

This incident highlights several important lessons and is a compelling case study for maritime cybersecurity education. First, it shows how cyberattacks can create operational immobility by bridging the digital-physical divide. Secondly, it emphasizes how intertwined port operations are, and how a security lapse in one area can quickly spiral into a major disruption. Lastly, it highlights the need for strong cybersecurity measures and skilled staff who are aware of the operational and technical ramifications of cyber threats, given that ports are vital hubs for international trade.

The Port of Houston, Texas, experienced a cyberattack in 2021 that targeted its computer network. Attackers tried to take advantage of a zero-day vulnerability in the software. The attack's characteristics indicated that a nation-state actor was involved, with the intention of obtaining confidential government data and possibly interfering with or stopping operations (Paganini, 2021). Because the Port of Houston handles almost half of all containerized cargo in the Gulf of Mexico and is a key hub for the US energy industry, the incident is especially significant from a strategic standpoint. The attackers' goals of gaining access to confidential government data and possibly interfering with operations highlight a troubling trend where ports are increasingly targeted as entry points to more extensive national security resources as well as for immediate disruption (Paganini, 2021).

An example of maritime cybersecurity flaws in action is the 2017 Black Sea GPS spoofing incident. This attack is especially concerning because of its scope where more than 20 vessels were impacted at once (GNSS, 2018). It became evident how easily highly skilled attackers could manipulate vital navigation systems that mariners trust when several ships unexpectedly discovered their GPS systems showing they were mysteriously located at an airport miles away. The Black Sea incident serves as a clear reminder that cybersecurity in the maritime environment is about more than just data protection; it's also about guaranteeing the basic safety of ships, crew, and cargo in a digital seascape that is becoming more and more contested.

A clear example of how cyber threats can halt even the most advanced maritime operations is the Lockbit ransomware attack on the Port of Nagoya in 2023 which sent shockwaves through the global supply chain as Japan's busiest port, handling more than 40% of the nation's trade volume (Lyngaas, 2023). This attack is especially notable because it targets automated container handling systems. The port's contemporary advantages turned into its biggest weaknesses when these systems were breached. The event shows how ransomware attacks have progressed from simple data encryption to calculated attacks on vital operational systems. Data from 2024 paints a picture of maritime cybersecurity challenges. There were 23,400 malware detections, 178 ransomware attacks, 50+ billion firewall events and 14. 8 billion security alerts. These numbers are increased dramatically compared to 2023 which shows the need for training and implementation of enhanced security measures (Marpoint, 2024).

Implementation of Maritime Education

Universities across the United States are slowly implementing maritime cybersecurity courses and degrees. A significant change in cybersecurity education that acknowledges the particular difficulties of protecting maritime infrastructure is indicated by the slow rollout of maritime cybersecurity degrees and courses. Academic institutions need to close the gap between traditional IT security and the unique requirements of the maritime industry as a result of increasingly complex digital threats against ports, ships, and global supply chains. Given the rising number of cyberattacks that target maritime operations, this advancement in education is critical. By incorporating maritime cybersecurity into university curricula, future cybersecurity professionals will be prepared with both industry-specific knowledge of safeguarding

shipboard systems, port networks, and critical operational technologies (OT) in addition to standard cybersecurity skills.

In March 2024 the University of North Carolina Wilmington announced that they will help to develop national standards and train the future workforce on how to protect America's marine transportation systems from cyber threats. The University secured a $625,000 grant from the federal budget for this development titled, "Maritime Cyber Security: Standards Advancement, Research and Workforce Development." This funding initiative's main objective is to strengthen the maritime subsector's security and resilience within the larger transportation systems sector. Maritime operations, one of the 16 critical infrastructure sectors identified by Presidential Policy Directive 21, are essential to both economic stability and national security. Efforts to improve cybersecurity, update security frameworks, and protect maritime assets from changing threats are supported by this funding (Guthrie, 2024).

The University of Plymouth offers maritime cyber threat mitigation training to meet the specific needs of the maritime sector. They offer one to five-day courses for groups to ensure a holistic approach to cyber risk management. Courses such as Maritime Cyber Threat Mitigation Awareness, Intermediate Maritime Cyber Threat Mitigation, Advanced Maritime Cyber Threat Mitigation or Mixed Team Scenario Training and Advanced Company-wide cyber security training. All courses align with the NIST Cybersecurity Framework. They are able to replicate systems of most of the world's shipping fleet in laboratory conditions (University of Plymouth, 2025).

In conjunction with the U.S. Coast Guard Cyber Command Maritime Cyber Readiness Branch, the USCG Office of Port and Facility Compliance and the USCG Sector NY, the Stevens Institute of Technology has developed a Maritime Cybersecurity professional development course tailored to the education needs of the USCG marine safety personnel (Stevens, 2025). The course is designed to provide a fundamental understanding of cybersecurity concepts within the context of the Maritime Transportation System (MTS). Texas A&M University at Galveston (2025) has a Maritime Cybersecurity Minor designed for both technical and non-technical students. The need to add this minor was due to the increase in reported attacks in the maritime industry that shut down electronic positioning systems on ships. At Rutgers University (2025) they offer a Maritime Risk Bootcamp which offers students hands-on experience through real-world projects. The students work with professionals in the field and work on projects with autonomous systems, the evolving landscape of cybercrime and maritime security and enforcement.

The development of these programs shows a growing understanding of the critical role maritime cybersecurity plays in both national security and international trade, even though adoption is still slow. The growth of specialized research, training initiatives, and industry collaborations will further establish maritime cybersecurity as a fundamental area of study in cybersecurity education as more academic institutions acknowledge the significance of this field. A skilled workforce that can protect the digital foundation of global trade is essential to the future of maritime cybersecurity.

Developing Maritime Cyber Curriculum

The development of maritime cybersecurity courses and programs is now urgently needed due to the increasing reliance on digital technologies in maritime operations and the growing number of cyber threats that target ports, vessels, and logistics networks. The vulnerability of global trade systems to cyber interference is exemplified by cyberattacks against maritime infrastructure, which can range from GPS spoofing and ransomware disruptions to operational technology (OT) breaches. The maritime industry faces

growing threats to efficiency, safety, and economic stability in the absence of specialized cybersecurity education. Below you will find recommended courses to include in University cybersecurity programs.

Foundations of Cybersecurity in Maritime Operations

This course offers a thorough introduction to cybersecurity concepts. Students will investigate fundamental cybersecurity ideas, threat scenarios, and defense tactics designed to address the particular weaknesses of maritime infrastructure, such as ships, ports, and supply chains

Cybersecurity Law and Policy

The legal and regulatory frameworks governing cybersecurity are examined in this course. Students will investigate how cybersecurity governance in international maritime operations is shaped by international cybersecurity laws, compliance standards, and policy developments. The course will cover topics such as liability, privacy laws, cyber risk management, and government reactions to cyberthreats in the maritime industry.

Cybersecurity Threats and Vulnerabilities in IT and OT Systems

This course examines how information technology (IT) and operational technology (OT) interact within critical infrastructure. In order to analyze the vulnerabilities that present security risks in the transportation, industrial, and maritime sectors, students will look at how these systems work both independently and dependently. Network security, threat detection, risk mitigation techniques, and real-world case studies of cyber incidents aimed at IT and OT environments will all be covered in the course.

Cybersecurity Risk in Maritime Operations

This course provides an in-depth exploration of cyber-physical risk assessment methodologies tailored to maritime systems. Students will analyze the vulnerabilities present in interconnected digital and operational technologies within ports, vessels, and maritime logistics. The course will emphasize risk identification, mitigation strategies, and resilience planning to protect maritime assets against cyber threats that could disrupt operations and global trade.

GPS and AIS Operations

This course examines the basic functions of Automatic Identification System (AIS) and Global Positioning System (GPS) technologies in maritime navigation, as well as the security risks associated with jamming and spoofing attacks. Students will study how these systems are used by ships for port arrivals, positioning, and collision avoidance, as well as how cyber threats can interfere with or take down these systems.

Economics of Port Operations

The economic concepts guiding port operations and their effects on international trade are thoroughly examined in this course. Students will investigate the financial, logistical, and policy-driven elements that affect ports' profitability and efficiency as vital hubs in global supply chains.

Maritime Supply Chain Management: Security, Operations and Logistics

With an emphasis on the interconnected networks that support international trade, this course examines the challenges of managing a maritime supply chain. The logistical, operational, and security issues that maritime transportation systems face such as port operations, cargo handling, and vessel routing will be examined.

Marinetraffic.com

MarineTraffic which can be found at martinetraffic.com (2025) has developed into a well-known platform for research and visualization of maritime data. It is dedicated to gathering and disseminating important maritime data and is based on international academic collaboration and developments in information and communication technology (ICT). This is an excellent site to expose students to understanding the global impact of the maritime and the global economy. Marinetraffic.com allows users to see the location of ships in real-time. The website provides both free and paid versions of the tool to monitor near real-time information regarding vessels' positions and movements as they relate to ports, traffic and voyage details across coastlines of most countries around the globe. Marinetraffic collects and presents data on the following:

- Marine telecommunications as they relate to efficiency and propagation parameters
- Simulation of vessel movements to assist with the navigation safety and to deal with critical incidents
- Provides real-time information
- Statistical processing of ports' traffic with applications in operational research
- Designed of efficient algorithms to determine the estimated arrival time of ships
- Correlates collected information with weather data

Figure 1 is an image that was taken from marinetraffic.com which each vessels location in a particular area. Students can gain a practical understanding of the intricacies of international maritime operations by using MarineTraffic.com which offers real-time insights into vessel movements. Students can get experience in the industry they are learning to secure by interacting with actual ship data, including routes, technical specifications and the country of origin. A deeper comprehension of logistical operations and cybersecurity vulnerabilities in maritime systems is fostered by this type of direct engagement.

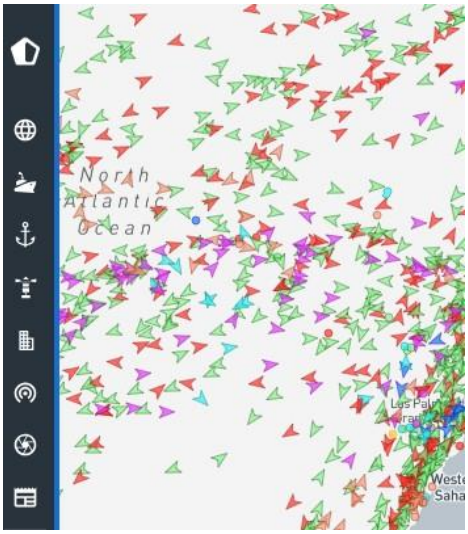

Figure 1. Image from MarineTraffic.com – Live active vessels

Studying vessel movements and operational details allows students to visualize potential cybersecurity risks. Examples of these risks include the significance of protecting automated tracking systems, avoiding data manipulation, and protecting navigational communications from cyber threats. They can examine digital infrastructure facilitates maritime logistics and analyze security issues beyond theory when real-world applications are incorporated into their coursework.

Methodology

The methodology used for this research is an extensive review of the literature. In order to investigate current trends, threats, and best practices in maritime cybersecurity, this study conducted a thorough literature review. To find recurrent themes and significant weaknesses in maritime digital infrastructure, a wide variety of scholarly journals, official documents, and technical standards were examined. To make sure the analysis included both established knowledge and new insights, sources were chosen according to their publication date, relevance, and credibility. A narrative review is an adaptable and descriptive technique that provides a thorough summary of a subject by synthesizing the body of existing literature. This method enables the researcher to investigate patterns, themes, and gaps across a wide range of sources rather than concentrating on rigorous inclusion criteria or methodical data analysis. Narrative reviews are especially helpful for setting the scene, showing how a field has developed, and pinpointing areas that require more study.

Results

By giving students specialized knowledge catered to the particular difficulties of maritime operations, integrating maritime cybersecurity into university curricula greatly improves the readiness and proficiency of students studying cybersecurity. The maritime industry necessitates a unique approach because of its dependence on automated port systems, operational technology (OT), and vessel navigation technologies. Conventional cybersecurity education frequently concentrates on general IT security. The below research question was examined for this study.

RQ1: *How can implementing maritime cybersecurity into university curricula improve the preparedness and expertise of students studying cybersecurity?*

The research has demonstrated that by adding maritime cybersecurity to university curricula it can greatly improve students' readiness and proficiency in the field. Students learn about the particular vulnerabilities of maritime infrastructure, such as shipping logistics, port operations, and vessel navigation systems, through the introduction of specialized coursework. This inclusion bridges the gap between traditional cybersecurity education and the industry-specific challenges faced by ports and vessels by providing students with practical skills suited to protecting maritime assets from cyber threats. Furthermore, exposure to practical case studies, practical instruction, and cooperation with stakeholders in the maritime sector enhance their capacity to evaluate risks, create security plans, and react to cyberattacks.

The reported cybersecurity incidents in the maritime sector highlight the growing susceptibility of the sector to online attacks and the pressing need for specialized training in the area. Both professionals and students can learn a great deal about the unique security issues that maritime operations face by examining real-world cyberattacks, such as GPS spoofing that interferes with vessel navigation or ransomware that targets ports. The maritime incidents provide compelling evidence of the pressing need for university cybersecurity programs to incorporate maritime cybersecurity. These events make for interesting case studies that draw attention to serious cybersecurity flaws in vessel infrastructure, operational technology (OT), and port systems. They also show why threat detection, risk mitigation, and realistic defense tactics specific to the maritime industry must be incorporated into maritime cybersecurity education in addition to traditional IT security.

Future cybersecurity professionals can be better prepared to safeguard national security interests, supply chain stability, and international trade by integrating lessons learned from previous cyber incidents into university curricula. The study emphasizes that, in a time of growing cyberthreats, maritime cybersecurity

education is not only advantageous but also necessary to guarantee the resilience of vital maritime infrastructure. Universities are essential in producing a trained workforce that can secure vital transportation systems as cyber threats targeting international maritime operations continue to increase. The study emphasizes how a comprehensive maritime cybersecurity curriculum can help protect global trade and maritime infrastructure from changing cyberthreats while also enhancing students' expertise.

Conclusion and Future Research

Given the increasing number of cyberthreats aimed at ports, ships, and international trade networks, the study highlights the need for maritime cybersecurity education. Universities are slowly realizing the need for specialized training in this area as a result of documented instances of cyber incidents impacting important maritime infrastructures. The industry-wide realization that cybersecurity knowledge must go beyond traditional IT security to cover maritime-specific threats is reflected in the steady rise in the number of institutions offering maritime cybersecurity courses. Research has also found possible course offerings that could improve maritime cybersecurity education. Specialized modules on cyber risk management for port operations, securing operational technology (OT) systems aboard ships, and applying advanced threat detection techniques in maritime logistics may be included in these courses.

Future research should concentrate on growing and enhancing maritime cybersecurity education in higher education. Evaluating the most effective teaching methods, curriculum, and industry collaborations to ensure that students receive relevant and practical education must be considered. Further research in these areas will strengthen the academic foundation for maritime cybersecurity, ensuring that graduates have the expertise needed to protect global maritime infrastructure. This research is necessary to create a workforce that is sustainable, prepared for the future, and able to lessen evolving cyberthreats.

References

Alcaid, J.K. & Llave, R.G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554

Alquarashi., F.S., Trichili. A., Saeed.N., Ooi.S., & Alouini. M.S. (2022). Maritime communications: A survey on enabling technologies, opportunities and challenges. IEEE Internet of Things Journal. *Vol. 10. No. 4. Pp. 3525-3547*.

Guthrie, G. (2024, April 11). UNCW to expand maritime cybersecurity program. University of North Caroloina Wilmington. https://uncw.edu/news/2024/04/uncw-to-expand-maritime-cybersecurity-program

I.GNSS. (2018). Reports of mass gps spoofing attack in the black sea strengthen calls for pnt backup. https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls/protect%20/discretionary%20%7B/char%20/hyphenchar%20/font%20%7D%7B%7D%7B%7Dfor-pnt-backup/

Ilascu, I. (2018) Port of barcelona Suffers Cyberattack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/port-of-barcelona-suffers-cyberattack/

Li, M., Zhou. J., Chattopadhyay, S., & Goh, M. (2024). Maritime cybersecurity: A comprehensive review. IEEE Transactions on Intelligent Transportation Systems zrXiv:2409.11417v3

Lyngaas, S.(2023, July 6). Japan's largest port hit with ransomware attack. CNN. https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack/index.html

M. Intelligence. (2024). Global port security market emerging trends and forecast. https://www.mordorintelligence.com/industry-reports/port-security-systems-market

Marpoint. (2024). 2024: A year of rising tides in maritime cybersecurity. https://marpoint.gr/blog/2024-a-year-of-rising-tides-in-maritime-cybersecurity/

Meland, P.H. Bernsmed, K., Froystad, C., Li, J., & Sindre, G. (2019). *An experimental evaluation of bowtie analysis for security.* Information and Computer Security.

Mrakovic., K & Vojinovic, R. (2019). Maritime cyber security analysis-how to reduce threats? Transactions on maritime science, 8(01), 132-139.

Nautic, P. (2025, April 25). *What is maritime? Definition and Meaning 2025* https://primonautic.com/blog/maritime-industry-global-trade/

Paganini, P. (2021, September 26). Port of Houston was hit by an alleged state-sponsored attack. Security Affairs. https://securityaffairs.com/122599/hacking/port-of-houston-cyberattack.html

Park, C. (2024). *Cybersecurity risk assessment in the maritime industry.* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ https://researchonline.ljmu.ac.uk/id/eprint/22728/1/2024%20Changki%20Park%20PhD.pdf

P.T. International. (2021). Digital maritime market worth $159 billion. https://www.porttechnology.org/news/digital-maritime-market-worth-159-billion/

Rutgers (2025). Experiential Learning for Business and Science. Maritime Risk Bootcamp. https://externship.rutgers.edu/externship-bootcamp/maritime-risk-bootcamps/

Stevens Institute of Technology (2025). U.S. Coast Guard Maritime Cybersecurity Course. https://www.stevens.edu/program/maritime-cybersecurity-course

Texas A & M University of Galvestgon (2025). Maritime Cybersecurity Minor

University of Plymounth (2025). Maritime cyber threat mitigation training. https://www.plymouth.ac.uk/research/cyber-ship-lab/maritime-cyber-threat-mitigation-training

Varley, T., Alhambra, E., B., Marisa, Kim, L., K. N., L, K., Traylor, S., Greene, S., Kardon, I., Reese., & Ashooh, E. (2024). *Shoring up maritime cybersecurity – Enhancing cybersecurity resilience.* DHS Office of Policy. 2024 Public-Private Atlantic Exchange Program